Claims

1. A system for sharing a random process between at least two separate parties, the system comprising at each party:

a primary bitstream, and

a selector for randomly selecting parts of said primary bitstream to form a random bit source,

wherein each selector is operable to use said random bit source to randomize said selection operation in an identical manner.

2. A system according to claim 1, wherein said primary bitstream is obtainable as a stream of bits from a data exchange process between said two parties.

3. A system according to claim 1, wherein said bits in said primary bitstream are separately identifiable by an address, and wherein said selector is operable to select said bits by random selection of addresses.

4. A system according to claim 1, wherein each selector comprises an address generator and each address generator is identically set.

5. A system according to claim 4, wherein each address generator is operable to make use of a random bitstream to randomize said addresses generation.

6. A system according to claim 1, further comprising a controller for exchanging control data between said parties to enable each party to determine that each selector is operating synchronously at each party.

7. A system according to claim 6, wherein said control data includes any one of a group comprising:

redundancy check data of at least some of the bits from said random bit source, and

a hash encoding result of at least some of the bits from said random bit source.

8 A system according to claim 6, wherein said control data includes any one of a group comprising:

redundancy check data of at least some of said addresses, and

a hash encoding result of at least some of said addresses.

9. A system according to claim 6, wherein said selector further comprises a resynchroniser operable to determine from said control data that synchronization has been lost between the parties and to regain synchronization based on a predetermined earlier part of the output of said random bit source.

10. A system according to claim 9, further comprising a backup data exchanger for exchanging said data for regaining synchronization.

11. A system according to claim 9, wherein said resynchronizer further comprises a backup data storage for storing previously exchanged data for regaining synchronization to be used for resynchronization with a party that has not made said exchange.

12. A system according to claim 9, wherein said resynchronizer is operable to create in advance future data to be used for resynchronization for resynchronizing with a party that has made said exchange in advance.

13. A random data generator, comprising

an input means for receiving a bitstream,

a random selector for selecting random individual bits from said bitstream to form a random data stream,

wherein said random selector is randomized by a previous segment of said random data stream.

14. A random data generator for reproducing a random data stream producible by an identical generator at another location, comprising

an input means for receiving a bitstream,

a random selector for selecting random individual bits from said bitstream to form a random data stream,

wherein said random selector is randomized by a previous segment of said random data stream.

15. A random data generator according to claim 14, wherein said bitstream is at least part of a data exchange process between parties associated with said generators.

16. A random data generator according to claim 15, further comprising a synchronization check unit for adding data to said data exchange process to enable a remote party to determine that it is producing an identical random data stream.

17. A random data generator according to claim 16, further comprising a resynchronization unit operable to use for resynchronization a predetermined earlier part of said random data stream upon receipt of an indication that said random data generator is not producing a random data stream that is identical to one being produced by said remote party.

18. A random data generator according to claim 17, wherein said resynchronization unit is operable to signal to said remote party upon carrying out said resynchronization.

19. A random data generator according to claim 18, wherein said resynchronization unit is operable to exchange said predetermined earlier part at predetermined intervals.

20. A random data generator according to claim 19, operable to define a gray area around said exchange, and within said gray area, to exchange control signals with said remote party to ensure that said parties use the same predetermined earlier part.

21. A method for sharing a random process between at least two separate parties, comprising the steps of:

obtaining at each party a primary data stream, and

randomly selecting parts of said primary data stream to form a random data source, and

using said random data source to randomize said selection operation in an identical manner at each party.

22. A method according to claim 21, wherein said primary data source is obtainable as a stream of bits from a data exchange process between said two parties.

23. A method according to claim 21, wherein said primary data source comprises a stream of data bits divisible into data units and comprising the step of selecting at random from the data bits of each data unit.

24. A method according to claim 23, wherein said bits in said data units are separately identifiable by an address, and comprising the step of selecting said bits by random selection of addresses.

25. A method according to claim 21, wherein said step of selecting is carried out by using identically set pseudorandom data generation at each party.

26. A method according to claim 21, further comprising the step of exchanging control data between said parties to enable each party to determine whether they are operating synchronously with said other party.

27. A method according to claim 26, wherein said control data includes any one of a group comprising:

redundancy check data of at least some of said random data source, and

a hash encoding result of at least some of said random data source.

28. A method according to claim 26, comprising the further steps of determining from said control data that synchronization has been lost between

the parties and regaining synchronization based on a predetermined earlier part of said random data source.

29. A method according to claim 28, further comprising a step of exchanging said data for regaining synchronization

30. A method according to claim 29, further comprising a step of storing previously exchanged data for regaining synchronization to be used for resynchronization with a party that has not made said exchange.

31. A system according to claim 29, further comprising a step of creating in advance future data to be used for resynchronization for resynchronizing with a party that has made said exchange in advance.